

Nine Things Employees Will Learn During User Awareness Training to Protect Companies from Cyber Breaches



1888 PressRelease - User awareness training by CipherEx educates employees about best practices for protecting themselves and their workplaces from cyber breaches.

ORINDA, Calif. - With cyber breaches happening to large corporations dominating the headlines, many small- to medium-size businesses are looking for ways to help protect themselves from falling victim. One of the easiest ways to help protect organizations is user awareness training. Simply put, user awareness training educates employees about best practices for protecting themselves and their workplaces.

According to CipherEx's (<http://www.CipherEx.com>) President and Founder, Siamak Behbahani, "There are nine primary areas that cover the basics of cyber security in the office, which even include the physical security of the office. Most employees are responsible and want to help protect their company; they just need the knowledge to be able to do so."

The user awareness course should cover a range of areas in which security practices are addressed. Below are a few of the areas that should be covered with employees:

- Security in the Office - Keeping the organization's workplace physically secure with proper use of access card keys is a critical component of security training.
- Password Security - From the building's front door to the smallest handheld device, understanding best practices for password use is vital to a business.
- Social Engineering - Learning to recognize a scam will keep employees from clicking on fraudulent links or falling for ploys that are designed to steal data.
- Securing Data - Every company should have a sound backup system for its data in case of system failures or natural disasters. Each employee must know the company's backup rules.
- Sharing Info/Social Networks - Social networks like Facebook and Twitter make it easy to overshare information, which could lead to a breach of company confidentiality and data.
- Internet File Sharing Services - Although highly convenient, file sharing services can lead to inadvertent sharing of confidential data, data corruption and delayed data transfers.
- Mobile Data Storage Devices - External components like flash drives, CDs and DVDs can transport malicious code into a network. Safety rules are essential.
- Data Destruction - Employees must be aware of the importance of shredding and destroying confidential information, even when it's outdated.
- Phishing/Spear Phishing - An urgent email from a seemingly legitimate source can be a ruse to gather important information, such as passwords, which allow access to the company's data.

Such security training courses should cover information such as these nine areas of training in a format that is easy for users to understand. Reviews and quizzes should be incorporated into the training to help make

sure that the employees have retained the information. Built-in testing techniques that allow IT managers to assess and review the learner's retention are a key component of any user awareness training system.

Behbahani added, "For end-user training to be effective, the people going through the program must understand and retain the information. Information in user awareness training should ideally be delivered in short sessions. In addition, the material must be easy to digest and learn without losing the user's interest. Short, individual video presentations with movement and sound allow employees to take courses at their own pace."

User awareness training is a simple step to make companies more secure. Learn more about CipherEx's user awareness training at <http://www.cipherex.com/awareness-training>.

About CipherEx

Since 2003, the people at CipherEx have been serving major global corporations with network and network security consulting, improving productivity and ROI in a more secure environment. The company's user awareness training covers key areas such as security in the office, password security, social engineering, securing data, sharing info/social networks, internet file sharing services, mobile data storage devices, data destruction and phishing/spear phishing in easy-to-understand video presentations that are a cost effective way to educate employees about cyber risks. To learn more, visit www.CipherEx.com.

###